UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

BLOCKCRUSHR INC., Plaintiff, v. CONSENSYS INC., CONSENSYS FUND I, L.P., CONSENSYS DILIGENCE, INC., CONSENSYS GP I, LLC, AND CONSENSYS VENTURES LLC, Defendants.	No. _____ **JURY DEMANDED**

COMPLAINT

Plaintiff, BlockCrushr Inc. brings this action against ConsenSys Inc., ConsenSys Fund I, L.P., ConsenSys Diligence, Inc., ConsenSys GP I, LLC, and ConsenSys Ventures LLC (collectively "Defendants"), and alleges as follows:

I. INTRODUCTION

1. This case concerns Defendants' misappropriation of Plaintiff BlockCrushr's trade secrets for its recurring payment systems enabled by smart contracts on the Ethereum blockchain.[1] Defendants, using their position of trust and posing as investors and mentors for BlockCrushr, misappropriated valuable trade secrets and launched an identical, competing product the day before BlockCrushr was set to publicly launch its product.

[1] As explained in further detail below, Ethereum, like Bitcoin, is a cryptocurrency characterized by a distributed ledger known as a blockchain.

2. In August 2018, BlockCrushr was a rising tech darling. It had just graduated from the prestigious Techstars startup incubator, had raised significant capital funding, and had hired its seventh employee. This momentum generated significant enthusiasm from potential customers—nearly 200 people signed up for news updates concerning its product launch. Its product, an Ethereum-based recurring payments solution, was seen as a promising solution that would allow Ethereum-based companies to generate revenue from its customers.

3. Then, on August 21, 2018, Defendants invited BlockCrushr to participate in its Tachyon accelerator program, which was specifically tailored to companies developing products involving the Ethereum blockchain. Defendants also offered to invest $100,000 in BlockCrushr, which BlockCrushr accepted. Under the terms of the investment, Defendants could request confidential information about BlockCrushr's business operations. In turn, Defendants were obligated to keep that information confidential and only utilize it to assess and guide BlockCrushr.

4. Defendants had a unique connection to the Ethereum ecosystem: its founder, Joseph Lubin, was a founding architect of the Ethereum blockchain. After launching Ethereum, Lubin founded ConsenSys AG, the umbrella company of the Defendants. ConsenSys plays an integral role in the Ethereum ecosystem as it is the largest developer of Ethereum-based applications in the United States, if not the world.

5. Throughout its Tachyon accelerator program, Defendants promised to open additional channels of funding for BlockCrushr to develop its product further and to integrate it into the Defendants' Ethereum-based ecosystem. To capitalize on this opportunity, founders Scott Burke and Andrew Redden and a number of their employees uprooted their lives and joined the Tachyon program in California in September 2018.

6. In the weeks that followed, the BlockCrushr team repeatedly met with Defendants, and, pursuant to a confidentiality agreement, detailed every aspect of its marketing, financial, technical, and regulatory strategy. BlockCrushr also shared its main asset: the source code and proprietary technical solution to its recurring payments platform. Defendants told BlockCrushr that they would protect BlockCrushr's trade secrets, and continually promised BlockCrushr more money and a bigger role in the Ethereum ecosystem—as long as BlockCrushr kept sharing.

7. These frequent conversations and meetings continued past the Tachyon accelerator program and through February 2019 when, without explanation, Defendants abruptly ceased their communications with BlockCrushr and its team. The additional funding and investments promised by the Defendants never materialized. Nevertheless, BlockCrushr pushed forward. Left without its anticipated partner and funding, BlockCrushr laid off employees and streamlined operations.

8. BlockCrushr pushed to get its product out to the marketplace as quickly as possible to bring on paying customers and generate revenue. Burke and Redden targeted an August 23, 2019 product launch. BlockCrushr negotiated new funding with a different investor. That funding was contingent on a successful product launch.

9. On July 23, 2019, BlockCrushr told Defendants of its planned product launch hoping to spur interest from its one-time partner.

10. BlockCrushr did not launch its product on August 23, 2019. Instead, on August 22, 2019, Defendants launched Daisy Payments, their own recurring payment management solution on the Ethereum blockchain. Defendants launched Daisy Payments by leveraging the trade secrets Burke and Redden disclosed during the Tachyon accelerator program.

11. Stunned, Burke and Redden reached out to Defendants to try and salvage the situation. Defendants were initially apologetic, telling Burke and Redden that its investment arm

would make sure this wouldn't happen in the future. Of course, this empty promise did nothing to undo the harm caused to BlockCrushr.

12. As explained in detail below, Daisy Payments is built off trade secrets Defendants deliberately misappropriated from BlockCrushr. This misappropriation destroyed BlockCrushr's ability to monetize its Ethereum-based recurring payments solution. This action is brought to rectify this injustice.

II. PARTIES

A. Plaintiff

13. BlockCrushr Inc., d/b/a Groundhog, is a federal corporation organized under the laws of Canada and headquartered in Halifax, Nova Scotia, Canada. It was founded by Scott Burke in February 2016. Andrew Redden joined as a co-founder in February 2017. While BlockCrushr is its formal company name, its trade name for the blockchain recurring payments business is Groundhog. The two names are interchangeable for the purposes of this Complaint.

B. Defendants

14. ConsenSys Inc. is a corporation organized under the laws of Delaware and headquartered at 48 Bogart Street Suite 22, Brooklyn, NY 11206. ConsenSys Inc. or a parent company markets and offers the "Codefi" suite of products, which includes Daisy Payments.

15. ConsenSys Fund I, L.P. ("ConsenSys Fund") is a limited fund partnership organized under the laws of Delaware and located at 48 Bogart Street Suite 22, Brooklyn, NY 11206.

16. ConsenSys Ventures LLC is a limited liability company organized under the laws of Delaware, and upon information and belief, located at 48 Bogart Street Suite 22, Brooklyn, NY 11206.

17. ConsenSys GP I, LLC ("ConsenSys GP") is a limited liability company organized under the laws of Delaware and located at 48 Bogart Street Suite 22, Brooklyn, NY 11206. ConsenSys GP I operates ConsenSys Fund.

18. ConsenSys Diligence, Inc. is a corporation organized under the laws of Delaware and headquartered at 48 Bogart Street Suite 22, Brooklyn, NY 11206. Upon information and belief, ConsenSys Diligence is owned wholly by ConsenSys Inc.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action raises a federal question under the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1831 *et seq*.

20. The Court has supplemental jurisdiction over BlockCrushr's other claims pursuant to 28 U.S.C. § 1367.

21. In addition, this Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332 as the parties are diverse in citizenship, and the amount in controversy exceeds $75,000.

22. Venue lies within this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to these claims occurred in this District. Nearly all Defendants are headquartered or reside in this district. The founder of ConsenSys AG, Joseph Lubin, resides in Brooklyn, New York. Lubin runs ConsenSys AG from Brooklyn where he oversees ConsenSys's operations, including the Tachyon accelerator program.

IV. FACTUAL ALLEGATIONS

A. The Beginnings of BlockCrushr

23. Burke and Redden are serial entrepreneurs who founded BlockCrushr for the same reason so many people start companies: they identified a problem, and then set out to solve it.

24. Their collaboration began in earnest during the Blockchain Virtual GovHack competitive "hackathon"[2] hosted by the city of Dubai in 2017. Burke pitched Redden on entering the competition to build out BlockCrushr's Hypergive product. The Hypergive product was designed to combat hunger amongst homeless individuals by leveraging blockchain technology. It accomplished this by providing "digital food wallets" that local community members could donate to. Those wallets would then be spent at local participating food retailers.

25. For this product, Hypergive received the 2017 Year of Giving Award at the World Government Summit in Dubai. Burke and Redden were flown to Dubai to receive the honor from the United Arab Emirate's prime minister. Encouraged by this success, Burke and Redden decided to commit themselves to building innovative blockchain-related products and services.

26. Through 2017 BlockCrushr continued its ascent as it developed new products relating to cryptocurrencies and blockchain technologies. It consulted with the United Nations and Microsoft on projects involving blockchain payments, artificial intelligence, and machine learning.

27. BlockCrushr's success in 2017 culminated in its acceptance into the prestigious Techstars incubator program.

B. Techstars and the Genesis of the Recurring Payments System

28. Techstars is a top startup incubator and accelerator which offers a three-month "bootcamp" for small cohorts of early-stage startup companies. It is notoriously competitive to get into, with less than 1% of applying companies making the cut.

29. During the bootcamp, the accepted startups work on all aspects of their business, attend classes, and make connections with others in the industry. Perhaps most importantly,

[2] A hackathon is an event that typically lasts for a short period of time – at most several days – where individuals collaborate to produce a prototype of an application or product.

Techstars' mentors and volunteers—drawn from a variety of executives and individuals with expertise in marketing, finance, business, and technology—provide personal mentorship and guidance.

30. If accepted into the program, Techstars also invests some "seed" money for a small (around 6%) stake in the company.

31. The program ends with a "demo day," where the accepted startup companies pitch the business to venture capitalists and other potential funders and partners. In part because they can pick the best startups, and in part because of the stamp-of-approval that comes with acceptance into the program, Techstars companies are widely successful. Some have achieved valuations north of a billion dollars. All told, Techstars companies have raised over $9 billion.

32. BlockCrushr applied for and was accepted into Techstars at a $3 million valuation. BlockCrushr began the bootcamp in January 2018.

33. Only weeks into the program, Burke and Redden identified a major pain point permeating BlockCrushr's prior products and which would form the basis of the trade secrets at issue in this case: the difficulty of obtaining recurring cryptocurrency payments for subscription or monthly services.

C. Bitcoin and Ethereum

34. A cryptocurrency is a digital asset designed to work as a medium of exchange and/or a store of value. Cryptocurrencies leverage a variety of cryptographic principles to secure transactions, control the creation of additional units, and verify the transfer of the underlying digital assets.

35. At its core, Bitcoin is a ledger that tracks the ownership and transfer of every bitcoin in existence. This ledger is called the blockchain.

36. Blockchains act as the central technical commonality across most cryptocurrencies. While each blockchain may be subject to different technical rules and permissions based on the preferences of its creators, they are typically designed to achieve a similar goal – decentralization.

37. Accordingly, blockchains are generally designed as a framework of incentives that encourages some people to do the work of validating transactions while allowing others to simply take advantage of the network. Cryptocurrencies like bitcoin accomplish this with validators that expend computational resources to solve a complex puzzle that rewards individuals in the form of newly minted bitcoin. This process is colloquially referred to as "mining." Cryptocurrencies can also be obtained from someone else. A number of financial exchanges offer the ability to buy cryptocurrencies with fiat currency, such as the U.S. dollar, or other cryptocurrencies.

38. In order to spend and use bitcoin,[3] users maintain a "digital wallet" which stores the public and private keys used to track ownership, receive, or spend cryptocurrencies. Typically, transfer fees and transfer time for cryptocurrency transactions are much lower than transfers of U.S. dollars in the conventional banking system.

39. Ethereum is another decentralized cryptocurrency, which was proposed in 2013 and formally launched in 2015. Lubin is one of the early founders of Ethereum.

40. Behind Bitcoin, Ethereum is the second-most popular cryptocurrency with a market cap of around $26.7 billion as of July 14, 2020. The Ethereum blockchain functions similarly to the Bitcoin blockchain insofar as its miners act as the validators of the network. Miners of the Ethereum blockchain are paid for their services in the form of newly minted ether. [4]

[3] The term "bitcoin" can refer to both a computer protocol and a unit of exchange. Accepted practice is to use the term "Bitcoin" to label the protocol, software, and community, and the term "bitcoin" to label the units of exchange.

[4] Similar to the distinction between "Bitcoin" and "bitcoin," "Ethereum" is the label for the protocol, software, and community, and the term "ether" is the label for the units of exchange.

41. Unlike Bitcoin's blockchain, Ethereum was designed to enable "smart contract" functionality. A smart contract is a program that verifies and enforces the negotiation or performance of a contract. Smart contracts can be self-executing and self-enforcing, which theoretically reduces the transaction costs associated with traditional contracting.

42. As an example of how a smart contract works, consider a situation where two people want to execute a hedging contract. They each put up $1,000 worth of ether. They agree that, after a month, one of them will receive back $1,000 worth of ether at the dollar exchange rate at that time, while the other receives the rest of the ether. The rest of the ether may or may not be worth more than it was at the beginning of the month.

43. A smart contract enables these two people to submit the ether to a secure destination and automatically distribute the ether at the end of the month without any third-party action. The smart contract self-executes with instructions written in its code which get executed when the specified conditions are met. In another example, one digital recording company uses smart contracts to automatically pay royalties on music that it sells licenses for.

D. BlockCrushr's Recurring Payment System

44. As cryptocurrencies like Bitcoin and Ethereum rise in popularity, developers have created tools to enable the cryptocurrency economy.

45. BlockCrushr developed a recurring payments system by leveraging smart contract protocols on Ethereum to enable vendors to accept one-time or subscription payments in a number of cryptocurrencies.

46. With credit cards, customers can easily sign up for services that incur a monthly charge, such as a cellphone bill or subscription to a newspaper. These recurring payments systems authorize merchants to automatically bill and charge customers monthly without the customer having to approve the payment each time.

47. Cryptocurrencies and blockchains do not have a recurring payments system built into them. BlockCrushr encountered this problem when attempting to build blockchain products with subscription services. Indeed, when attempting to monetize its previous suite of blockchain products, BlockCrushr had to manually identify and bill each user's digital wallet, and even then, there was no guarantee a user would pay.

48. Soon after entering the Techstars program, BlockCrushr set out to solve this problem. It created a smart contract system that would allow merchants to automatically charge user's digital wallets, in return for a small transaction fee. This smart contract platform was comprised of both technical and business-orientated trade secrets, including:

a) Market and financial analysis, including analysis of the total addressable market, the competitive landscape, expected sales cycles and revenue, and a go-to-market plan for identifying and acquiring customers;

b) Customer information, including lists of customers, "early adopter" customers lists, and customer survey responses that informed product desirability, design, and launch strategy;

c) Regulatory and legal analysis, to understand how to technically structure products to account for money transmitter and other related laws;

d) Product design and strategy of current and future versions of the platform;

e) Technical design for structuring the digital wallets and smart contracts in order to successfully navigate the fraught regulatory system;[5] and

f) Almost 120,000 lines of source code, developed and modified over years. This source code was comprised of:

[5] BlockCrushr designed a system that whitelisted charges from a vendor under specific business logic that would trigger a payment from a merchant gateway. This solution prevented BlockCrushr from acting as a custodian over the funds or digital wallet and thus falling under money transmitter laws.

i. The technical system architecture and wallet to enable all aspects of the product, as well as designs for meta-transactions and relayers.[6] Technical designs included methods to scale its payment operations to handle a high volume of transactions.

ii. Customer and merchant dashboards which interact with BlockCrushr's smart contracts and transaction relayer. The dashboard provides a web interface for merchants and consumers to manage their wallet, subscriptions and payments.

iii. A payment widget for merchants to use BlockCrushr to allow them to cryptographically sign for the subscription payment with a wallet of their choice. The widget mediates the checkout flow for the user and communicates with BlockCrushr.

iv. A module to enable integrations between BlockCrushr and popular e-commerce product WooCommerce. The module mediates the checkout process and translates between BlockCrushr and WooCommerce events, processes, and business logic. In effect, the module enables merchants using WooCommerce to add a simple "Pay with Groundhog" option.

49. BlockCrushr developed many of these trade secrets while participating in the Techstars program. Their success in identifying the problem and coming up with a solution led to a successful Techstars demo day in April 2018. Less than a month after the demo day, BlockCrushr had commitments for additional funding at a valuation of $4 million.

50. At the time, BlockCrushr faced no competition, and no one else in the market was developing a recurring payments solution for blockchain-based payments. Indeed, when promoting BlockCrushr's Groundhog product in September 2018, ConsenSys admitted that "Pre-authorized, recurring payments aren't possible with today's crypto wallets and payment gateways, and Groundhog is building the technology to enable this huge category of payments for the new world of decentralized finance."

[6] Meta-transactions and relayers allow users to interact with certain Ethereum applications without directly paying the Ethereum transaction cost for interacting with the Ethereum blockchain.

51. Groundhog conducted market surveys and other outreach, and prospective customers repeatedly shared their enthusiasm for BlockCrushr's product as a way to help them monetize their own projects. One customer survey described BlockCrushr's Groundhog product as "ingenious." Another explained how he was "really interested in learning how to receive crypto recurring payments." Still another gushed that "[w]hat really drew me into researching more about Groundhog though is the subscription-based service. That allows me to focus on building my product instead of the subscription system. It looks fantastic and I am excited to see Groundhog develop."

E. At all Times, BlockCrushr Took Reasonable Measures to Keep Information Secret

52. BlockCrushr took security very seriously. Not only did it understand that its intellectual property was its largest asset, BlockCrushr also understood that its role in the cryptocurrency payment industry made it a target. Cryptocurrency companies had historically and famously been the target of major thefts and hacking, and BlockCrushr worked hard to design systems to ensure its systems were safe.

53. BlockCrushr hosted their source code on the secure platform BitBucket,[7] which used industry-leading encryption for its communications with BlockCrushr (for example, when BlockCrushr uploaded code). Only BlockCrushr employees—and then later, ConsenSys employees—had access to the company's BitBucket repository. Access to the repository was segmented by role and logged.

[7] BitBucket is a cloud-based software version control company. It allows companies to securely and collaboratively work on code and keep track of the latest version of code through a system of checking in and out code.

54. BlockCrushr also implemented a dual system of two-factor authentication.[8] At the first level, each employee account could only be accessed using both a password and a Google verification system. Next, BlockCrushr implemented a hardware authentication security module. Even after successfully logging on, employees could only access the company's servers with a physical key plugged into their laptop. Employee's laptops were also encrypted with 256-bit keys.

55. BlockCrushr employees, consultants, and contractors were required to sign non-disclosure agreements when they joined the company.

56. BlockCrushr employees and contractors were instructed not to share proprietary information outside of the company.

F. BlockCrushr's First Interactions with Defendants

57. Burke and Redden first met with individuals associated with the ConsenSys[9] umbrella of companies on May 18, 2018, at an event for developers and partners of the Ethereum blockchain. At that event, Redden and Burke met ConsenSys employee John Packel, who in turn introduced them to Kavita Gupta, head of ConsenSys Ventures. ConsenSys Ventures is the venture capital arm of ConsenSys, investing in pre-seed and seed-stage Ethereum blockchain projects.

58. ConsenSys was founded in early 2015 by Lubin—one of the founders of the Ethereum protocol. ConsenSys bills itself as a "market-leading blockchain technology company" that promotes the Ethereum ecosystem by fostering the development of decentralized software services and applications that operate on the Ethereum blockchain. Accordingly, ConsenSys took

[8] Two-factor authentication is a method in which a user is granted access to some system or device only after successfully presenting two or more pieces of evidence of rightful access, such as unique knowledge (e.g., a password) or unique possession (e.g., a key).

[9] The Complaint will refer to "ConsenSys" and "Defendants" interchangeably at times because Defendants did not always differentiate between their different business units.

significant interest in the recurring payments solution BlockCrushr was developing, as it offered a powerful monetization solution for other Ethereum-based products and services.

59. In the months that followed, BlockCrushr and ConsenSys came to an agreement. ConsenSys would invest $100,000 in BlockCrushr in its latest $4 million valuation round. In addition, BlockCrushr would enter ConsenSys's Tachyon accelerator program. Given the positive experience BlockCrushr had with Techstars and Tachyon's Ethereum focus, BlockCrushr believed the accelerator program would be perfect for taking their business to the next level.

G. ConsenSys Agrees to Protect BlockCrushr's Trade Secrets

60. On or about September 5, 2018, as part of its acceptance into the Tachyon accelerator program, BlockCrushr signed a Convertible Equity Instrument (drafted by Defendant ConsenSys Fund, and attached hereto as Exhibit A), entitling ConsenSys Fund to invest up to $100,000 across several Convertible Equity Instruments in BlockCrushr. BlockCrushr would sign two more Convertible Equity Instruments with ConsenSys Fund, on October 22, 2018 (Ex. B) and November 4, 2018, (Ex. C), respectively. The terms of all three Convertible Equity Instruments are materially identical.

61. The Convertible Equity Instruments provide rights to ConsenSys Fund in exchange for its investment, including shares of BlockCrushr and the right to purchase more shares in the future.

62. The Convertible Equity Instruments also obligate BlockCrushr to provide certain information to ConsenSys, and in return ConsenSys would maintain the confidentiality of that information, using the information only for its role as an investor.

63. Specifically, the Convertible Equity Instruments state under Section 5.1(a):

> The Company [*i.e.*, BlockCrushr] shall provide ConsenSys with the following additional rights: To the extent that the Company prepares Financial Statements, the Company shall deliver to ConsenSys such Financial Statements upon request

> . . . . Additionally, regardless of whether the Company prepares Financial Statements, the Company shall deliver to ConsenSys such information relating to the financial condition, business or corporate affairs of the Company as ConsenSys may from time to time reasonably request. . . **ConsenSys agrees to maintain the confidentiality of all of the information provided to it under this Section 5.1(a) and agrees not to use such information other than for a purpose reasonably related to ConsenSys' investment in the Company**.

Ex. A at 6-7 (emphasis added).

64. On or about the same day as it entered into the first Convertible Equity Instrument, the parties entered into a Management Rights Letter. (Ex. D). Under this Management Rights Letter, ConsenSys Fund was granted additional rights, including, for example, the rights to (1) "consult with and advise management of the Company on significant business issues;" (2) "examine the books and record of the Company;" and (3) "designate a representative to serve on the Board of Directors of the Company." Ex. D at 1-2.

65. Gupta told Burke and Redden that ConsenSys negotiated for representation on the Board of Directors because BlockCrushr would join the ConsenSys family and become the default recurring payments service provider and board representation would help that integration.

66. Like the Convertible Equity Instruments, under the Management Rights Letter, "ConsenSys agrees . . . that it will keep confidential and will not disclose, divulge, or use for any purpose (other than to monitor its investment in the Company) any confidential information obtained from the Company pursuant to the terms of [the Management Rights Letter . . . ." Ex. D at 6.

67. Moreover, the Management Rights Letter explicitly binds all ConsenSys entities that received confidential information. The Management Rights Letter allows ConsenSys to disclose "**confidential information . . . to any existing or prospective affiliate, partner, member, stockholder, or wholly owned subsidiary of ConsenSys in the ordinary course of**

business, provided that ConsenSys informs such person that such information is confidential and directs such person to maintain the confidentiality of such information." Ex. D at 6.

H. BlockCrushr Discloses Trade Secrets as Part of the Tachyon Accelerator Program Pursuant to the Confidentiality Provisions of the Convertible Equity Instruments and the Management Rights Letter

68. Contracts in hand, the Tachyon 2018 accelerator program kicked off on September 7, 2018. Burke, Redden, and five other members of the BlockCrushr team uprooted their lives and moved to San Francisco, California for the program. At the time, they were excited and confident about building a collaborative relationship with ConsenSys.

69. The luster on the Tachyon accelerator program tarnished almost immediately, however, when BlockCrushr learned that they would not be receiving the entire $100,000 promised at once. The Convertible Equity Instruments call for an investment "up to" $100,000 and ConsenSys represented to BlockCrushr that the money was all but assured. Then, as BlockCrushr entered the program, Defendants held back nearly the entire amount, citing the need for additional "diligence." BlockCrushr would not see the first $10,000 until September 17, 2018.

70. Further, once BlockCrushr arrived in California, ConsenSys began to demand frequent, in-depth meetings about BlockCrushr's technology. These were disruptive to BlockCrushr's daily operations, but the company felt obligated to appease Defendants. Further, the BlockCrushr team thought that ConsenSys wanted to conduct diligence to ensure the product was real and could do what it claimed, because no other company had a similar solution yet.

71. Unlike the meetings and classroom activities with Techstars, where Burke and Redden felt like students learning from those more experienced, Burke and Redden largely became teachers. ConsenSys demanded that Burke and Redden disclose every facet of BlockCrushr's business and the innovative technology underpinning its recurring payments solution.

72. The meetings were constant. The following timeline details a representative overview of the substance of these interviews:

a. **September 12, 2018**: BlockCrushr and the rest of the entrants in that year's Tachyon class had a kickoff dinner with Joseph Lubin.

b. **September 12, 2018**: Redden and Burke met with Joseph Chow and Goncalo Ca from the ConsenSys Diligence team. Chow and Ca requested and received an in-depth examination of all aspects of BlockCrushr's technology, including technical trade secrets regarding system architecture design, wallet design, wallet interactions, meta-transactions and relayers, and smart contracts. This included code snippets, group discussion, and white boarding of concepts.

c. **September 13, 2018**: Redden and Burke met with Patrick Berarducci from ConsenSys legal. Berarducci asked Redden and Burke to explain BlockCrushr's trade secrets regarding its business model, legal and regulatory risks implicated by the technology, and the company's positioning to avoid them. Further, BlockCrushr explained the structure of the digital wallets and smart contracts to ensure a non-custodial system. Berarducci would become the Global head of FinTech for ConsenSys and lead ConsenSys Codefi, the division responsible for eventually launching Daisy Payments.

d. **September 14, 2018**: Redden and Burke met with Terry Rossi of ConsenSys Ventures. During the meeting, they shared trade secrets regarding their smart contract design, system architecture, application programming interface and meta-transactions.

e. **September 18, 2018:** Redden and Burke met with Miles Jennings from Latham and Watkins, LLP, counsel for ConsenSys. During that meeting, BlockCrushr revealed trade secrets regarding how to technically structure their smart contracts and architecture to avoid regulatory issues. The conversations were designed to be detailed enough to allow Latham and Watkins to provide a formal legal opinion on BlockCrushr's product.

f. **September 18, 2018:** Redden and Burke met with two representatives from Token Foundry, a ConsenSys division that helped blockchain companies raise funding through initial coin offerings.[10] Numerous Daisy Payments founding members worked at Token Foundry at this time before joining Daisy Payments, including Daisy Payments CEO and founder Patricio López Juri, Pedro Kompen, Joaquin Moreira, Vincente Dragicevic Hernández, and Nate Chastain. ConsenSys required Tachyon participants to meet with Token Foundry. During this meeting, Redden and Burke disclosed trade secrets, including the architecture of BlockCrushr's payment system, its customer pipeline, and its competitive market research. BlockCrushr did not know it at the time, but the Token Foundry project was struggling financially, and would be entirely abandoned within the next few months, with ConsenSys looking to reassign its employees elsewhere.

g. **September 19, 2018**: Redden and Burke met with Jerome De Tychey, Blockchain Technical Lead at ConsenSys. During this meeting, they disclosed trade secrets,

[10] An initial coin offering (ICO), similar to an initial public offering (IPO), typically allows companies to issue cryptocurrencies that users can purchase and then use with the company's services or sell on the secondary market.

presenting the technical architecture behind their payments system, including non-custodial wallets, subscription whitelisting, meta-transactions and relayer design.

h. **October 16, 2018:** Redden and Burke met with Joseph Lubin, founder of ConsenSys. They gave Lubin a progress update on the development of their platform and business development efforts, and they talked about the need for subscriptions for projects in the ConsenSys ecosystem.

i. **ConsenSys Ventures Meetings**. BlockCrushr's team had at least seven meetings with ConsenSys Ventures employees, including Gupta, between September 12 and November 14, 2018. The first meeting, on September 12, was with Gupta and Rune Bentien. In this meeting, Gupta first told Burke to not talk to investors. Prior to the meeting, Burke had requested an email introduction to a relevant investor, David Namdar, who had presented during the Tachyon accelerator program. Gupta demanded that Burke refrain from talking to investors prior to Tachyon's demo day. Burke pushed back at this notion, as this was contrary to the investor pipeline building strategy they had been taught during the Techstars program. Gupta insisted, with the promise of investor interest after Tachyon's demo day.

73. BlockCrushr had other meetings at Defendants' request too. For example, because its product was designed to enable blockchain companies to charge for services on a singular or recurring basis, BlockCrushr was seen as a critical solution for ConsenSys and Tachyon companies to generate revenue. Indeed, BlockCrushr was expected and promised to become a key cog in the ConsenSys and Ethereum machine.

I. Demo Day and Post-Demo Day Investment Discussions

74. Heading into Tachyon's demo day, Defendants assured BlockCrushr that the event would be well-attended by investors and luminaries in the blockchain and cryptocurrency space.

In fact, invitations were supposedly at such a premium that, upon information and belief, none of the investors Burke sought invitations on behalf of received invitations. BlockCrushr was looking forward to a well-attended demo day because ConsenSys had repeatedly advised BlockCrushr not to speak to outside investors during the program—an odd request for a supposed startup accelerator. BlockCrushr understood that, in return for complying with these requests, BlockCrushr was to be made a central pillar to the ConsenSys ecosystem. BlockCrushr relied on this promise in not aggressively pursuing other investors.

75. On November 16, 2018, BlockCrushr pitched at Tachyon's demo day. While fewer investors attended the demo day than promised, BlockCrushr felt encouraged when ConsenSys Ventures continued to express an interest in maintaining and growing the relationship with BlockCrushr.

76. Just a few days after the demo day, Burke and Redden spoke with Andreas Wallendahl, the founder of "Strategic Initiatives" at ConsenSys, about ConsenSys investing further in BlockCrushr. Wallendahl made two requests: (1) a lengthy due diligence call for a deep dive on BlockCrushr's product and (2) complete access to BlockCrushr's source code.

77. Discussions began in earnest. Between November 20, 2018 and February 27, 2019, BlockCrushr had at least sixteen meetings with members of the ConsenSys Ventures team to discuss an ongoing relationship.

78. On November 28, 2018, the Parties had a lengthy due diligence call recommended by Wallendahl. ConsenSys attendees included Alan Krassowski, Eli Geschwind, Patrick Berarducci, Wee Ming Choon, David Merin, and Joyce Lai. During this call, Burke and Redden went in-depth on all aspects of the company's product, technology, and business.

79. On November 29, 2018, Defendants requested further in-depth legal, financial, product, and technical details about BlockCrushr. Specifically, Defendants requested:

a. Technical information and access to the code;

b. Financial information, including historical cash flow, 2019 revenue projections, and monthly revenue per customer;

c. Product development goals and timelines;

d. Market strategy, including information on sales cycles, expected monthly recurring revenue, customer pipeline, and customer acquisition strategy;

e. Market analysis, including any materials on the competitive landscape and the addressable market; and

f. Regulatory and legal work product.

80. By November 30, 2018, BlockCrushr had materially complied with these requests, including granting ConsenSys access to the BitBucket repositories hosting BlockCrushr's source code.

81. Conversations continued, with eight additional due diligence meetings in January 2019. During those meetings, BlockCrushr continued to share and discuss detailed financial, marketing, and technical information.

82. Throughout January 2019, Redden spoke repeatedly, via messages and video calls, with Bernhard Mueller, a senior engineer at ConsenSys Diligence, and Vincente Dragicevic Hernández, an engineer at Token Foundry. During these meetings, they elicited information about how BlockCrushr worked. For example, Mueller and Hernández were interested in BlockCrushr's use of meta transactions to execute several sub-transactions at a higher scale than would be otherwise possible. Hernández also solicited information on how to uniquely identify transactions and invoices, and how to handle subscription cancellations. All of the information Redden shared were trade secrets of BlockCrushr.

83. Mueller assured Redden that these calls were to ensure that BlockCrushr was compatible with ConsenSys's smart contract auditing product, MythX, which ConsenSys wanted to monetize with subscriptions. Mueller was responsible for the MythX product. While Redden was confident that BlockCrushr could be used to implement subscriptions to MythX, ultimately the opportunity never arose.

84. On January 23, 2019, Redden met with Mueller to discuss BlockCrushr's technology and business plan in further detail.

85. On January 29, 2019, Mueller published a blog entitled "Bringing Mainstream E-Commerce to the Ethereum Blockchain." The post promised the development of an "open source . . . recurring payments [platform that] provide[d] a dapp frontend with a frictionless user experience." The product was to be called "Bouquet" and would be built by ConsenSys's Token Foundry division.

86. Within days of this blogpost, on February 4, 2020, Hernández copied part of BlockCrushr's publicly available code[11] into his own personal folder on GitHub.[12] And within weeks of the calls with Mueller and Hernández, Hernández would go on to become a founding member of Daisy Payments as a "Smart Contracts Engineer." Thus, during Daisy Payments' critical early development period, Hernández was receiving BlockCrushr trade secrets, asking questions of BlockCrushr, and looking at BlockCrushr's code.

[11] This code was used to mediate the subscription whitelisting and transaction approval and processing. It was built upon an open-source smart contract wallet. Smart contract code, when compiled, is publicly available as it must exist on the blockchain for public execution. While the public code is not part of BlockCrushr's asserted trade secrets described above, the logic and reasoning behind the design and its role within the larger system are trade secrets.

[12] https://github.com/vdrg/smart-wallet

87. Shortly after Mueller posted this article, ConsenSys abruptly ceased its due diligence meetings with BlockCrushr.

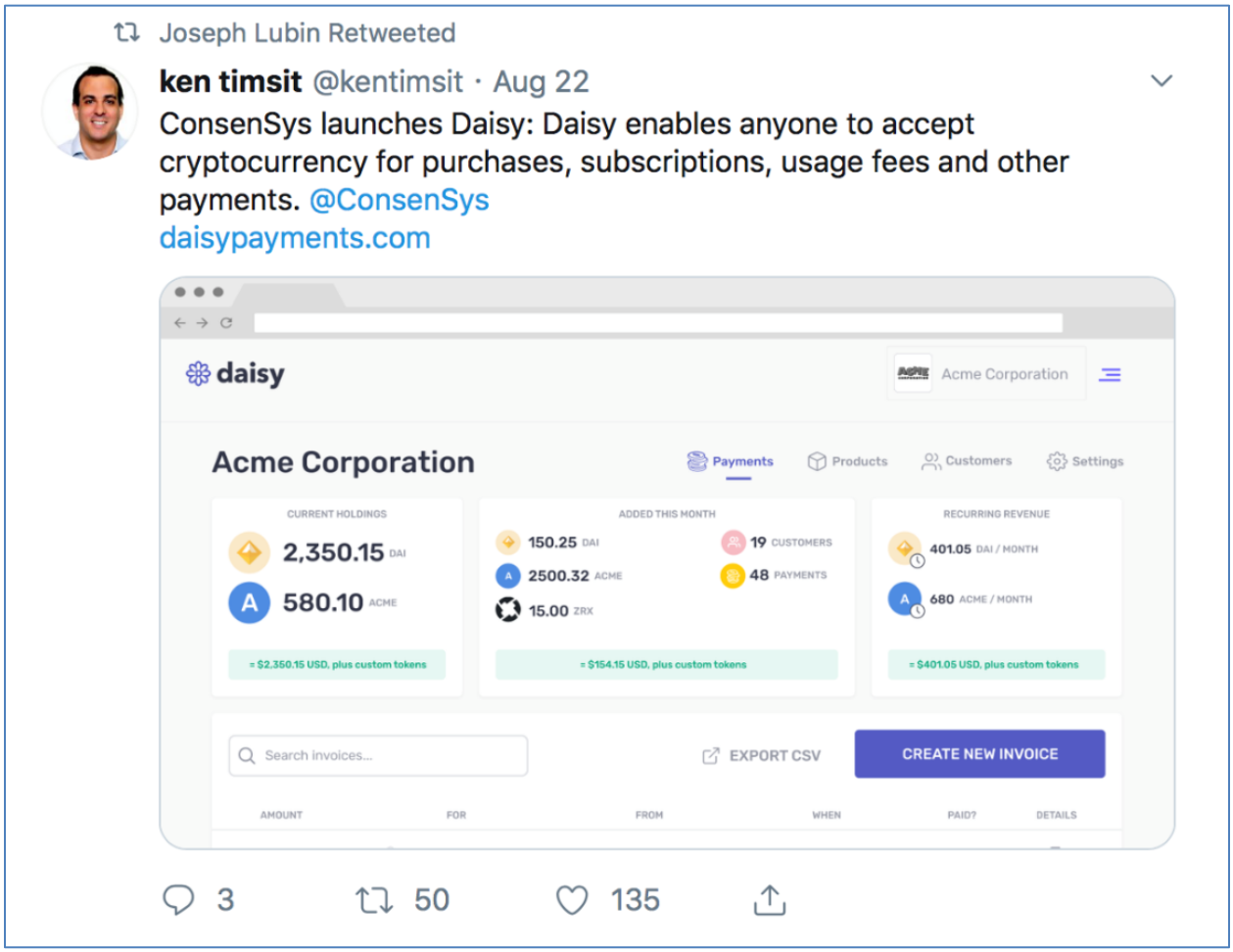
88. Months later, when BlockCrushr needed emergency financing to meet payroll obligations, Defendants ignored communications from Burke and Redden.

89. While Burke and Redden were troubled by the silence, BlockCrushr moved forward and planned to launch its recurring payments product on August 23, 2019. The launch would allow it to generate revenue by onboarding paying customers who were clamoring for the recurring payments solution. In conjunction with this launch, BlockCrushr secured another badly-needed round of funding at a $6 to $8 million valuation—contingent on reaching certain business milestones.

90. Hoping to remain on good terms with ConsenSys, on July 23, 2019 BlockCrushr sent its investors, including Defendants, an email announcement of its impending August 23, 2019 platform release date. BlockCrushr specifically highlighted its goal to use this launch as a springboard to raise another round of funding in "September or October," explaining that the launch "will be critical to closing the [funding] round."

J. Daisy Payments Launches the Day Before BlockCrushr

91. On August 22, 2019, one day before BlockCrushr was set to launch, ConsenSys launched Daisy Payments, a platform allowing "anyone to accept cryptocurrency for purchases, subscriptions, usages fees and other payments." In effect, it offered the identical product that the BlockCrushr team had been developing for the prior 19 months, since February 2018. Joseph Lubin himself promoted the launch to his over 100,000 Twitter followers.



92. Daisy Payments, was somehow envisioned, founded, and launched in less than half that time. Its website, www.daisypayments.com, was not registered until March 4, 2019—around the same time that Defendants stopped responding to BlockCrushr's communications.

93. According to his LinkedIn profile, Daisy Payments founder and CEO, Patricio López Juri, worked at Token Foundry until January 2019.

94. According to publicly available source code available at the code repository Github,[13] Juri did not start developing the code for Daisy Payments until February 2019. Other

[13] Companies, such as BlockCrushr and Daisy Payments, often make the part of its source code that its customers integrate into their product publicly available. This source code is only part of what these companies develop.

team members at Token Foundry began working on the precursor to Daisy Payments at this time as well.

95. As explained above, Token Foundry was a company under the ConsenSys umbrella designed to support the launching of ICOs on the Ethereum blockchain. Indeed, up until January 21, 2019, Token Foundry's website stated that it "set out last year to be the best platform for running initial coin offerings."

96. However, within just a few days of Mueller's blog post, Token Foundry announced that, instead of focusing on ICOs, it was pivoting to focus on "cryptocommerce." When Daisy Payments launched, another member of Mueller's ConsenSys Diligence stated that "for Ethereum, a suitable model for subscription payments didn't exist. So, working with our friends at Daisy Payments, **we built one**."

97. This was a sham.

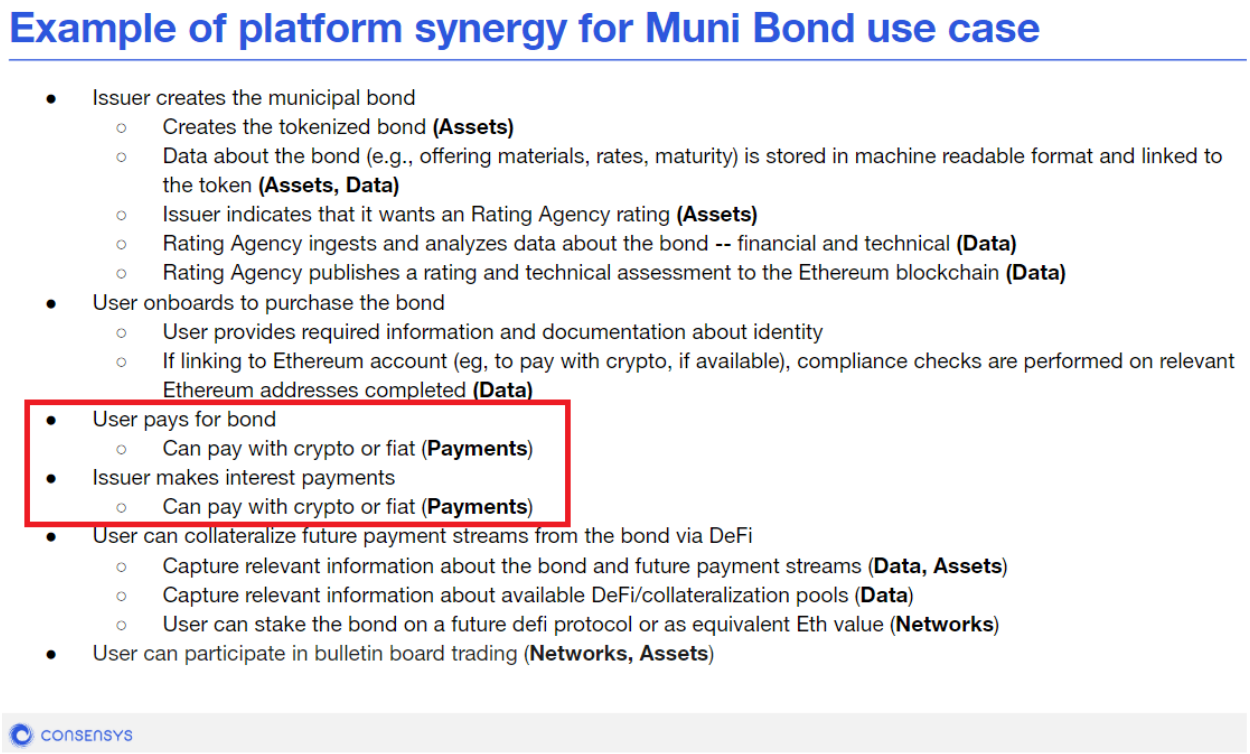
98. Daisy Payments was built by leveraging trade secrets that Defendants misappropriated from BlockCrushr and disclosed to the Daisy Payment's founders in violation of the Confidentiality Provisions of the Convertible Equity Instruments and Management Rights Letter. Notably, Daisy Payments' first customer was MythX, the ConsenSys product that Mueller was in charge of. Beyond using Daisy Payments for its standard subscription plan, MythX "also utilizes Daisy for enterprise products which require custom subscription plans."

99. At least six members of Daisy Payment's founding team came from Token Foundry and were Defendants' employees prior to starting Daisy Payments. At least one of them, Vincente Dragicevic Hernández, spoke directly with Redden about BlockCrushr's trade secrets.

100. Defendants' months long "due diligence" was a coordinated effort to unlawfully take BlockCrushr's trade secrets. Defendants never intended to invest further capital to help

BlockCrushr grow, nor did they intend to promote its recurring payments solution for use throughout the Ethereum ecosystem.

101. Since its launch, Daisy Payments has been rebranded as "CodeFi Payments" under ConsenSys AG as part of ConsenSys's global financial infrastructure offering, CodeFi. It is an integral customer acquisition tool and component for the CodeFi suite of products. For example, in February 2020, ConsenSys purchased Heritage Financial Systems, a broker/dealer focused on municipal bond issuance. With this purchase, ConsenSys hopes to "tokenize" municipal bond offerings in smaller denominations to allow municipalities to raise funds from a broader part of the community. Critically, as explained in detail during a ConsenSys presentation at the virtual Ethereal Conference in May 2020, ConsenSys will utilize its Codefi software to power this business. ConsenSys detailed in a separate slideshow that it will use Codefi Payments to power recurring interest rate payments:



Example of platform synergy for Muni Bond use case

- Issuer creates the municipal bond
  - Creates the tokenized bond **(Assets)**
  - Data about the bond (e.g., offering materials, rates, maturity) is stored in machine readable format and linked to the token **(Assets, Data)**
  - Issuer indicates that it wants an Rating Agency rating **(Assets)**
  - Rating Agency ingests and analyzes data about the bond **--** financial and technical **(Data)**
  - Rating Agency publishes a rating and technical assessment to the Ethereum blockchain **(Data)**
- User onboards to purchase the bond
  - User provides required information and documentation about identity
  - If linking to Ethereum account (eg, to pay with crypto, if available), compliance checks are performed on relevant Ethereum addresses completed **(Data)**
- User pays for bond
  - Can pay with crypto or fiat (**Payments**)
- Issuer makes interest payments
  - Can pay with crypto or fiat (**Payments**)
- User can collateralize future payment streams from the bond via DeFi
  - Capture relevant information about the bond and future payment streams (**Data, Assets**)
  - Capture relevant information about available DeFi/collateralization pools (**Data**)
  - User can stake the bond on a future defi protocol or as equivalent Eth value (**Networks**)
- User can participate in bulletin board trading (**Networks, Assets**)

CONSENSYS

K. Post-Launch Communications

102. On August 23, 2019, the day of BlockCrushr's planned release, Burke emailed Lubin to request a call to understand what impact the launch of Daisy Payments would have on ConsenSys's role as an investor in BlockCrushr. Burke knew that ConsenSys's sudden entry into the market would deflate investor enthusiasm in BlockCrushr, as a supporting pillar of the ConsenSys ecosystem suddenly became a competitor. And as a struggling, cash-strapped startup, without additional funds from investors or the expected support from ConsenSys, BlockCrushr would find it difficult to generate enthusiasm and offer a competitive product.

103. Lubin responded later that day, apologizing for the "confusion" and claiming he was not "aware of the potential conflict" although he admitted to tracking the projects "at a very high level." He promised to get back to Burke.

104. On September 13, 2019, Burke and Redden spoke with Praneeth Srikanti, a Principal at ConsenSys Ventures. During that call, Srikanti admitted he was "as shocked as" Burke and Redden.

105. Srikanti also admitted that ConsenSys made a mistake with the firewalls it was supposed to have in place to prevent BlockCrushr's assets from being used by other teams. He apologized, and said that ConsenSys Ventures was trying to make sure that the situation does not happen again. Srikanti gave explicit instructions for Burke and Redden to only discuss BlockCrushr-related updates with himself and a colleague from that day forward, for fear of more leakage to Daisy Payments.

106. By October 2019, Defendants had ceased all communications with Burke and Redden.

V. CAUSES OF ACTION

FIRST CAUSE OF ACTION
Misappropriation of Trade Secrets Under the Defend Trade Secrets Act
18 U.S.C. § 1836, et seq.
(Against All Defendants)

107. BlockCrushr incorporates herein by reference each and every allegation contained in the preceding paragraphs of this Complaint, and further alleges as follows:

108. BlockCrushr is the owner of valuable trade secrets related to products and services used in, or intended for use in, interstate or foreign commerce. Such trade secrets comprise BlockCrushr's financial, business, scientific, technical, economic and engineering information, including but not limited to, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs and codes, both tangible and intangible and stored, compiled and memorialized physically, electronically and graphically.

109. BlockCrushr has taken reasonable measures to keep such information secret.

110. BlockCrushr's trade secrets derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

111. Defendants disclosed and/or used BlockCrushr's trade secrets without BlockCrushr's express or implied consent. Defendants used improper means to acquire knowledge of the trade secrets by failing to abide by the confidentiality provisions of the Convertible Equity Instruments and Management Rights Letter.

112. Defendants knew or had reason to know at the time of disclosure or use that their knowledge of the trade secrets was derived from or through BlockCrushr and that Defendants used improper means to acquire the trade secrets. Defendants acquired the trade secrets under circumstances giving rise to a duty to maintain the secrecy of the trade secrets or limit the use of

the trade secrets. Defendants owed a duty to BlockCrushr to maintain the secrecy of its trade secrets or limit use thereof.

113. Defendants' improper means in disclosing BlockCrushr's trade secrets include Defendants' misrepresentation, breach or inducement of a breach of a duty to maintain secrecy of the trade secrets and breach of the confidentiality provisions of the Convertible Equity Instruments and Management Rights Letter.

114. Defendants, with intent to convert trade secrets that are related to a product or service used or intended for use in interstate or foreign commerce to the economic benefit of BlockCrushr, and intended or knowing that the offense will injure BlockCrushr, did knowingly the following:

a. stole, or without authorization, removed, concealed, or by fraud, artifice, or deception obtained such information;

b. without authorization copied, duplicated, sketched, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, or conveyed such information;

c. received or possessed such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

d. attempted to commit any offense described in paragraphs (a) through (c); or

e. conspired with one or more other persons to commit any offense described in paragraphs (a) through (c), and one or more of such persons performed an act to effect the object of the conspiracy.

115. Defendants continue to misappropriate BlockCrushr's proprietary information through continued sales of Daisy Payments and CodeFi Payments and development of these

blockchain subscription payment-related products. As a result of such misappropriation, BlockCrushr has suffered damages in an amount to be determined at trial.

SECOND CAUSE OF ACTION
Misappropriation of Trade Secrets
(Against All Defendants)

116. BlockCrushr incorporates herein by reference each and every allegation contained in the preceding paragraphs of this Complaint, and further alleges as follows:

117. BlockCrushr is the owner of valuable trade secrets related to products and services used in, or intended for use in, interstate or foreign commerce. Such trade secrets comprise BlockCrushr's financial, business, scientific, technical, economic and engineering information, including but not limited to, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs and codes, both tangible and intangible and stored, compiled and memorialized physically, electronically and graphically.

118. BlockCrushr has taken reasonable measures to keep such information secret.

119. BlockCrushr's trade secrets derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information. BlockCrushr derives an economic advantage of its competitors from its trade secrets.

120. Defendants had access to BlockCrushr's trade secrets pursuant to BlockCrushr's disclosure as part of the investor relationship as defined by the Convertible Equity Instruments and Management Rights Letter.

121. Defendants disclosed and/or used BlockCrushr's trade secrets without BlockCrushr's express or implied consent. Defendants used improper means to acquire knowledge of the trade secrets by failing to abide by the confidentiality provisions of the Convertible Equity Instruments and Management Rights Letter and otherwise.

122. Defendants knew or had reason to know at the time of disclosure or use that their knowledge of the trade secrets was derived from or through BlockCrushr and that Defendants used improper means to acquire the trade secrets. Defendants acquired the trade secrets under circumstances giving rise to a duty to maintain the secrecy of the trade secrets or limit the use of the trade secrets. Defendants owed a duty to BlockCrushr to maintain the secrecy of its trade secrets or limit use thereof.

123. Defendants' improper means in disclosing BlockCrushr's trade secrets include Defendants' misrepresentation, breach or inducement of a breach of a duty to maintain secrecy of the trade secrets and breach of the confidentiality provisions of the Convertible Equity Instruments and Management Rights Letter.

124. Defendants, with intent to convert trade secrets that are related to a product or service used or intended for use in interstate or foreign commerce to the economic benefit of BlockCrushr, and intended or knowing that the offense will injure BlockCrushr, did knowingly the following:

a. stole, or without authorization, removed, concealed, or by fraud, artifice, or deception obtained such information;

b. without authorization copied, duplicated, sketched, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, or conveyed such information;

c. received or possessed such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

d. attempted to commit any offense described in paragraphs (a) through (c); or

e. conspired with one or more other persons to commit any offense described in paragraphs (a) through (c), and one or more of such persons performed an act to effect the object of the conspiracy.

125. Defendants continue to misappropriate BlockCrushr's proprietary information through continued sales of Daisy Payments and CodeFi Payments and development of these blockchain subscription payment-related products. As a result of such misappropriation, BlockCrushr has suffered damages in an amount to be determined at trial.

THIRD CAUSE OF ACTION
Breach of Contract
(Against ConsenSys Fund and ConsenSys GP)

126. BlockCrushr incorporates herein by reference each and every allegation contained in the preceding paragraphs of this Complaint, and further alleges as follows:

127. ConsenSys Fund is a signatory to the Convertible Equity Instruments and Management Rights Letter, each a contract. ConsenSys GP manages ConsenSys Fund, executes contracts on its behalf, and is ultimately liable for any misconduct of ConsenSys Fund.

128. The Convertible Equity Instruments and Management Rights Letter each constitute a valid and enforceable written contract with definite and certain terms.

129. BlockCrushr has performed and is still performing all of its required obligations under both the Convertible Equity Instruments and Management Rights Letter.

130. As stated above, among other provisions, ConsenSys Fund and ConsenSys GP breached the confidentiality provisions of the Convertible Equity Instruments and Management Rights Letter.

131. As a result of the violation of the confidentiality provisions of the Convertible Equity Instruments and Management Rights Letter, BlockCrushr has suffered damages in an amount to be determined at trial.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment as follows:

i. A judgment that Defendants misappropriated BlockCrushr's trade secrets as alleged herein.

ii. A judgment that Defendant ConsenSys Fund and ConsenSys GP breached the valid, enforceable Management Rights Letter and Convertible Equity Instruments as alleged herein.

iii. Damages, including treble damages, assessed against Defendants pursuant to the Defend Trade Secrets Act of 2016, 18 U.S.C. § 1831 *et seq.*

iv. Damages assessed against Defendants for misappropriating trade secrets, including compensatory damages, unjust enrichment, or restitution damages and reasonable royalty damages.

v. Imposition of a constructive trust for the benefit of BlockCrushr as a vehicle for disgorgement of all monies, profits and gains Defendants have obtained or will unjustly obtain in the future at the expense of BlockCrushr.

vi. A grant of a permanent injunction to eliminate the unfair advantage Defendants gained by using BlockCrushr's trade secrets and other intellectual property.

vii. Punitive damages for Defendants' willful and wanton misappropriation and the tortious conduct described above.

viii. Exemplary damages pursuant to the Defend Trade Secrets Act for Defendants' willful and malicious conduct.

ix. Expenses, costs, and attorneys' fees.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury for all claims.

Dated: July 14, 2020
New York, New York

/s/ Kyle Roche

Kyle W. Roche
Richard R. Cipolla (*admission pending*)
Warren Li
ROCHE CYRULNIK FREEDMAN LLP
99 Park Street, Suite 1910
New York, New York 10016
(646) 791 6881

Attorneys for Plaintiff